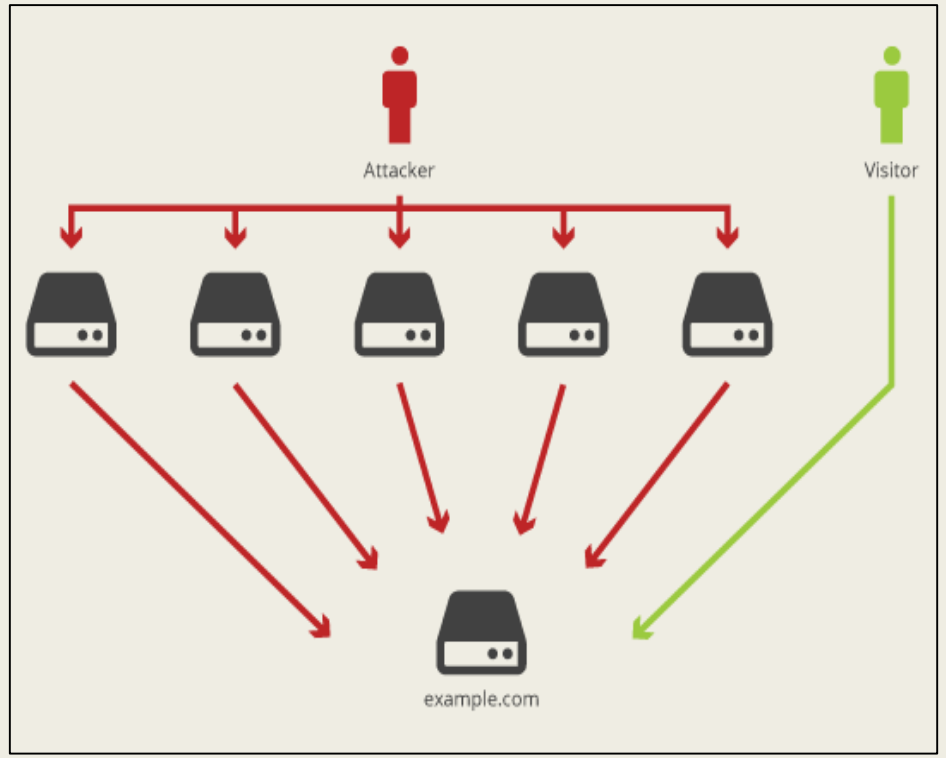
DDoS Attack
(Distributed Denial of Service)

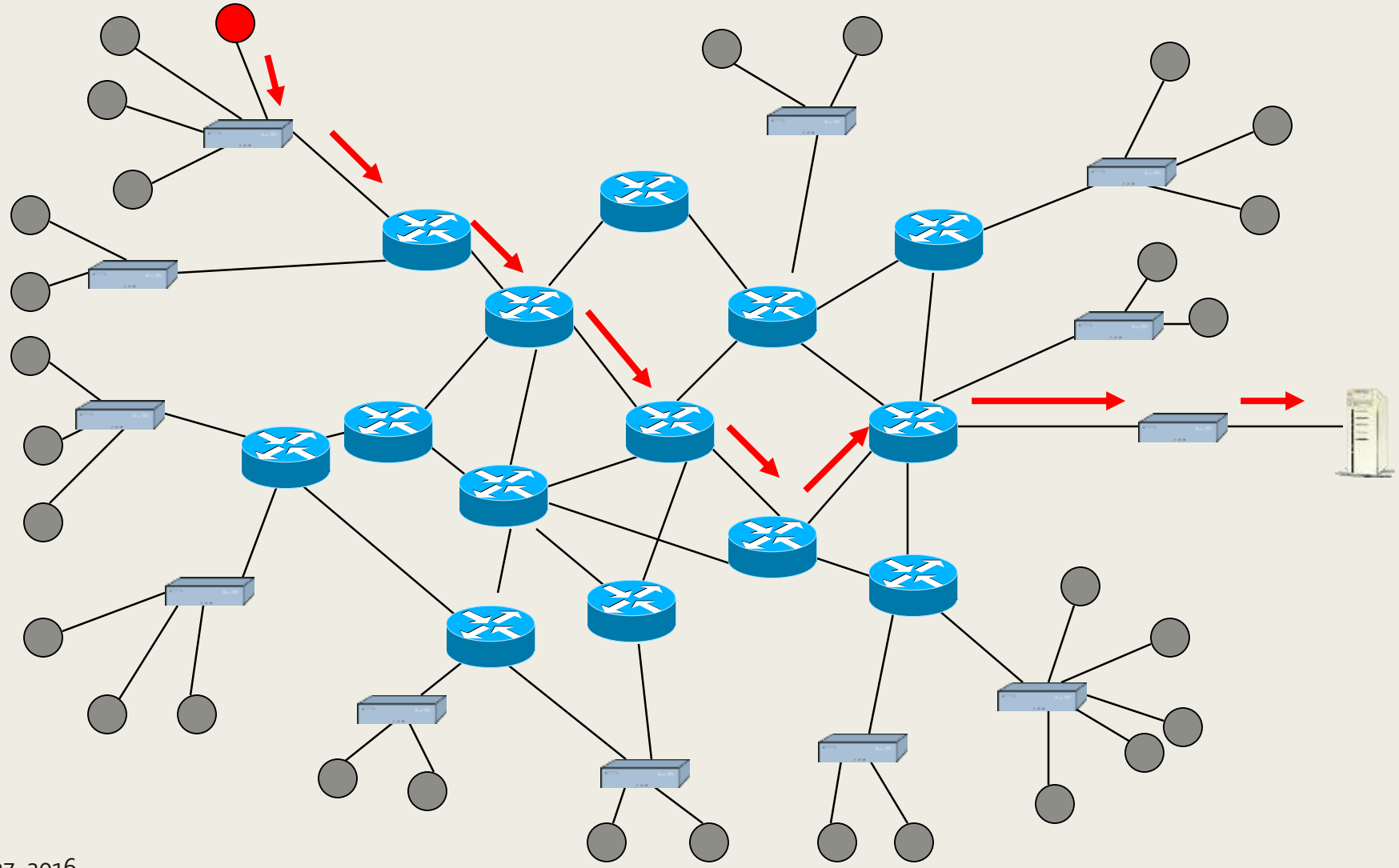
Er. Shiva K. Shrestha
Er. Niran Kafle

Introduction

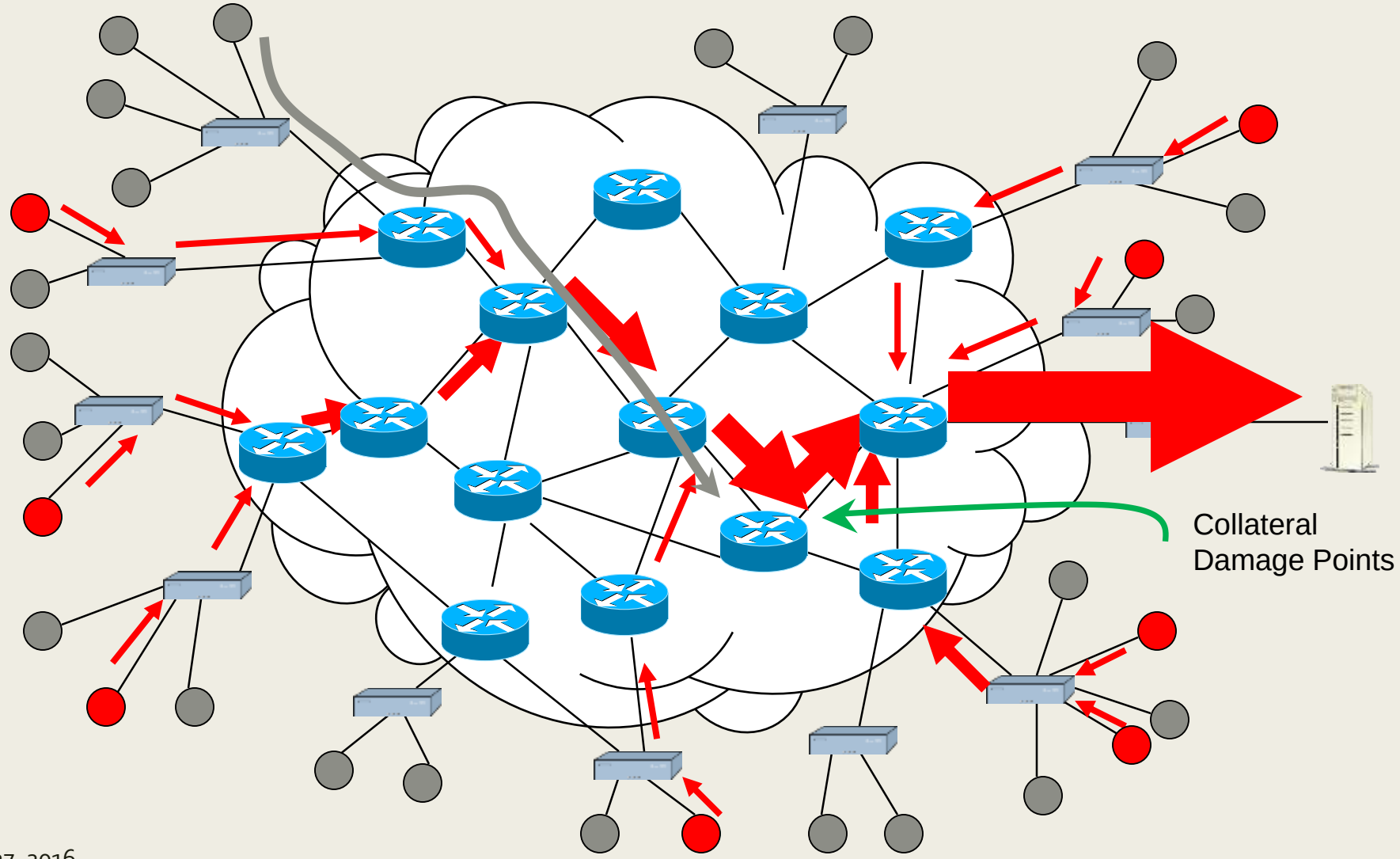
- Denial of Service (DoS)
  - *Attack to disrupt the authorized use of networks, systems, or applications*
- Distributed Denial of Service (DDoS)
  - *Employ multiple compromised computers to perform a coordinated and widely distributed DoS attack*
- DoS Attacks Affect:
  - *Software Systems*
  - *Network Routers/Equipment/Servers*
  - *Servers and End-User PCs*



DoS Single Source

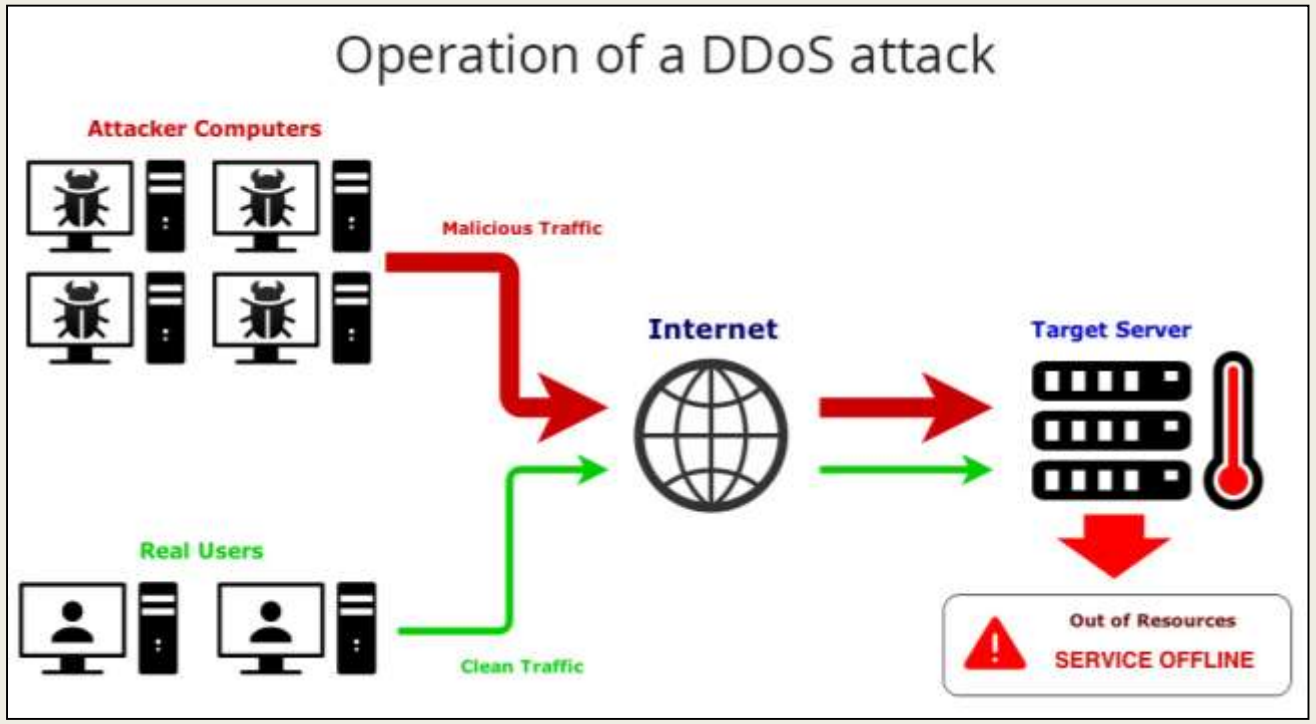


DDoS



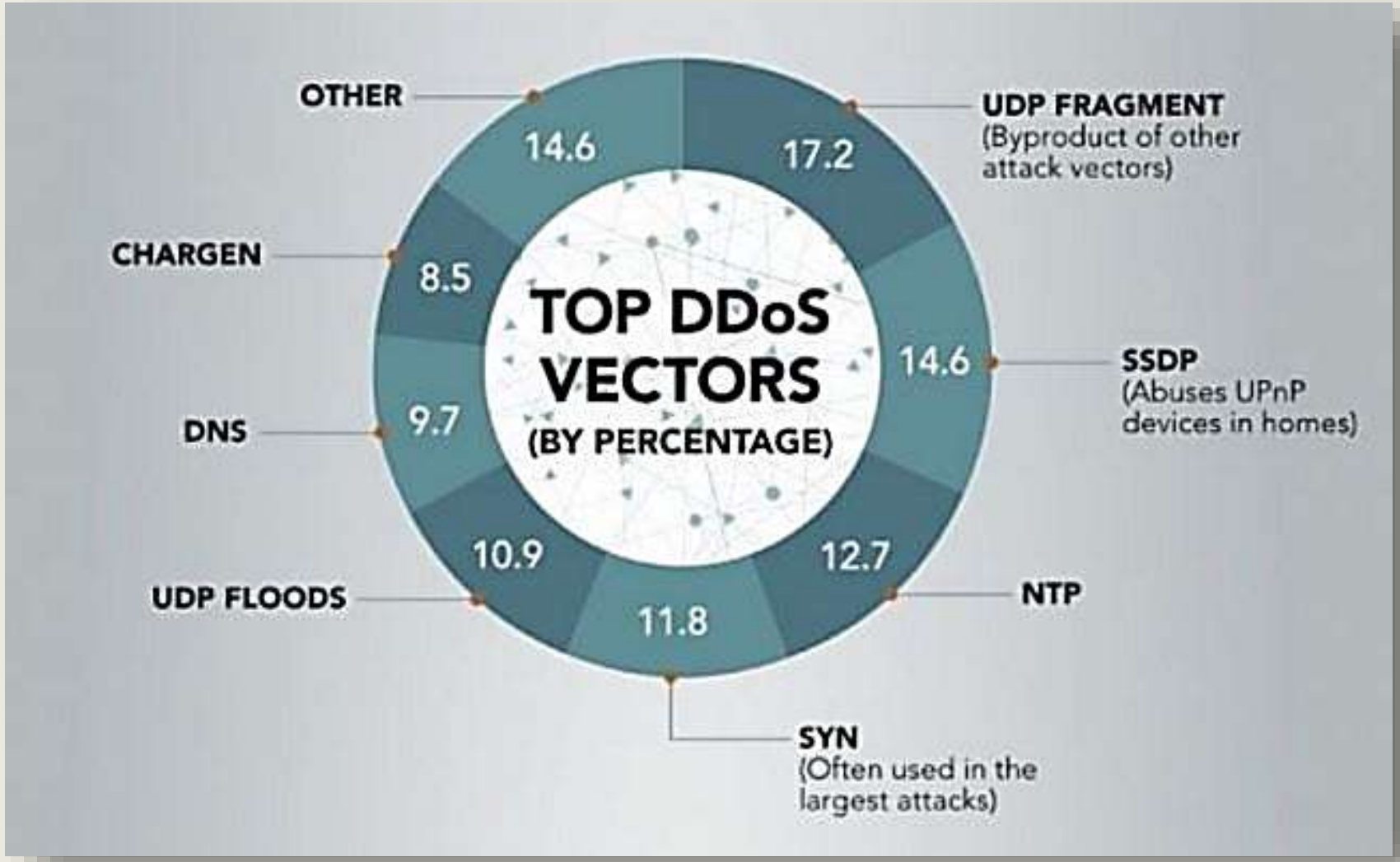
How DDoS Attacks Work

- incoming traffic flooding the victim originates from many different sources – potentially hundreds of thousands or more.
- effectively makes it impossible to stop the attack simply by blocking a single IP address;
- very difficult to distinguish legitimate user traffic from attack traffic when spread across so many points of origin.

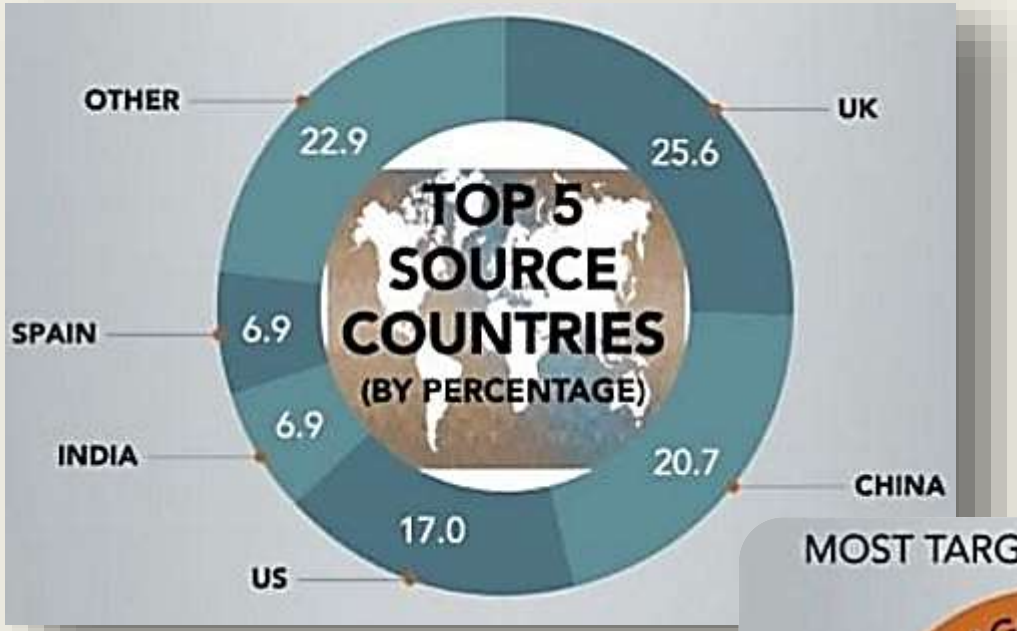


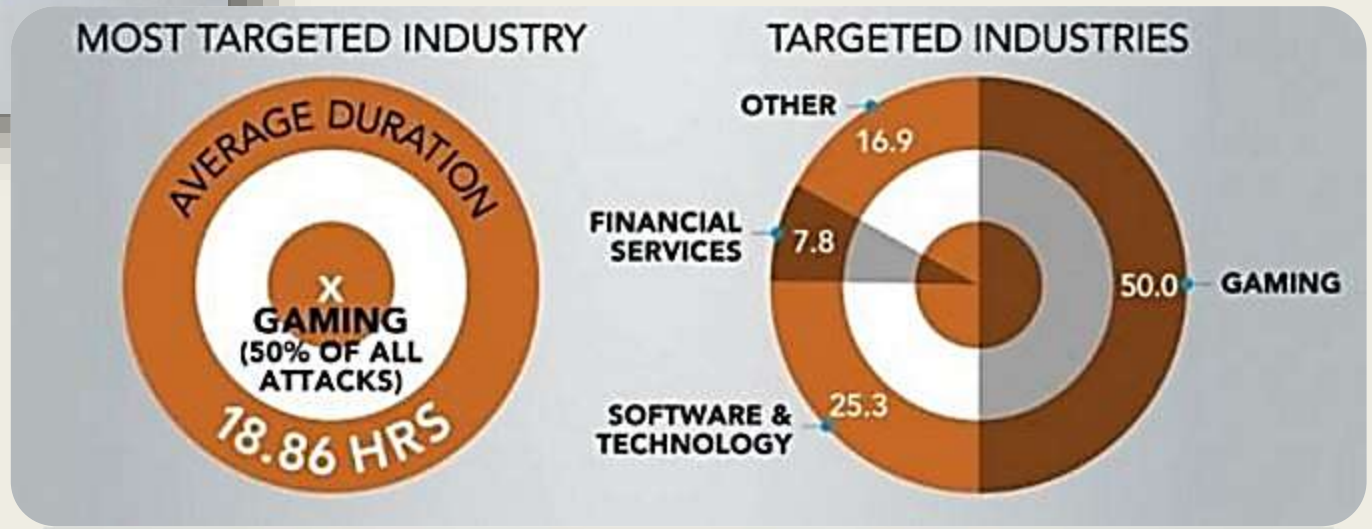
DDoS Headlines

DDoS Attacks Based On

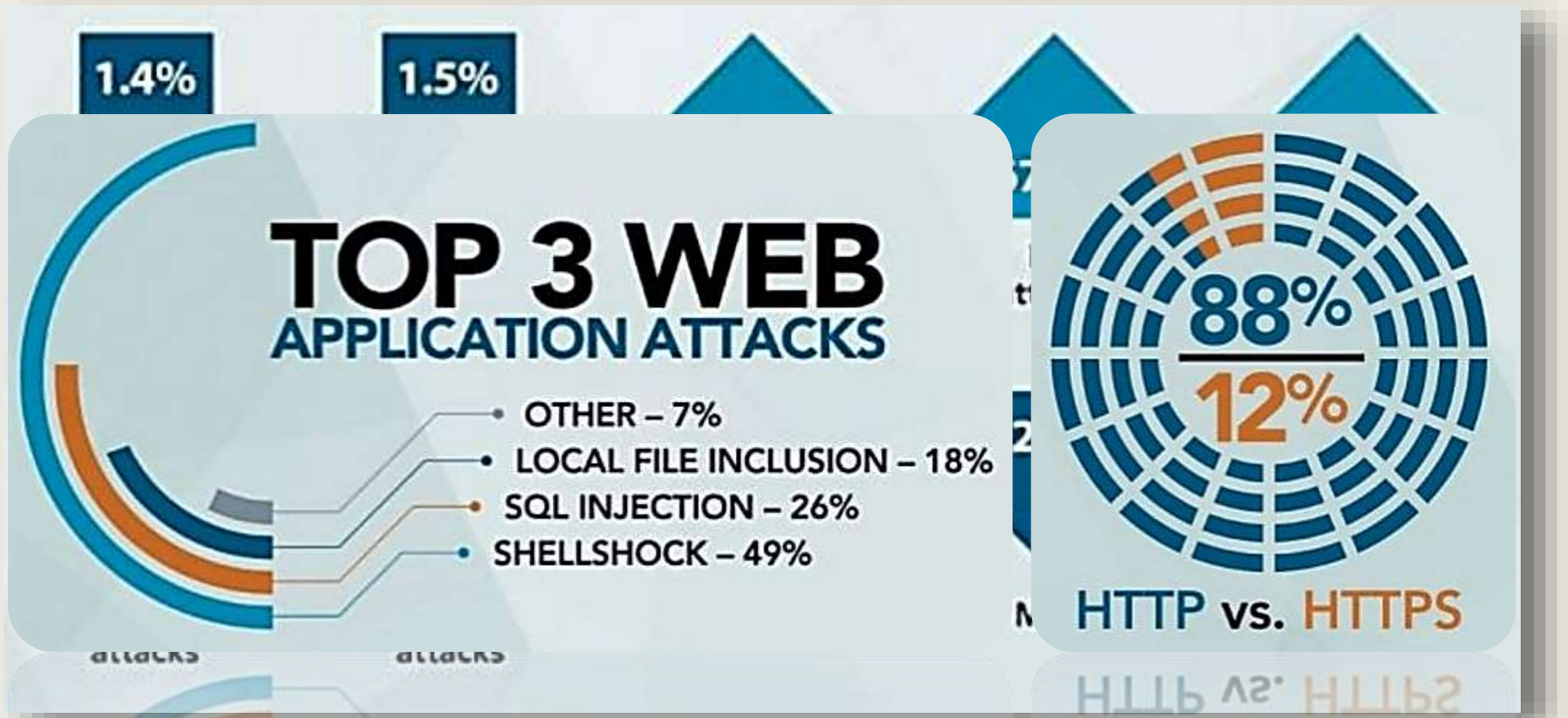


DDoS Source & Targets





DDoS Web Application Attacks



Types of DDoS Attacks

- **Traffic attacks:** Traffic flooding attacks send a huge volume of TCP, UDP and ICPM packets to the target. Legitimate requests get lost and these attacks may be accompanied by malware exploitation.
- **Bandwidth attacks:** This DDoS attack overloads the target with massive amounts of junk data. This results in a loss of network bandwidth and equipment resources and can lead to a complete denial of service.
- **Application attacks:** Application-layer data messages can deplete resources in the application layer, leaving the target's system services unavailable.

DoS Attacks Fast Facts

- Early 1990s: Individual Attacks single source. First DoS Tools
- Late 1990s: Botnets, First DDoS Tools
- Feb 2000: First Large-Scale DDoS Attack
  - CNN, Yahoo, E*Trade, eBay, Amazon.com, Buy.com
- 2001: Microsoft's name sever infrastructure was disabled
- 2002: DDoD attack Root DNS
- 2004: DDoS for hire and Extortion
- 2007: DDoS against Estonia
- 2008: DDoS against Georgia during military conflict with Russia
- 2009: Ddos on Twitter and Facebook
- 2010: Ddos on VISA and Master Card

2000 DoS Attacks

- In Feb 2000, series of massive DoS attacks
  - *Yahoo, Amazon, eBay, CNN, E*Trade, ZDNet, Datek and Buy.com all hit*
- Attacks allegedly perpetrated by teenagers
- Used compromised systems at UCSB
- Yahoo : 3 hours down with $500,000 lost revenue
- Amazon: 10 hours down with $600,000 lost revenue

NetworkWorldFusion

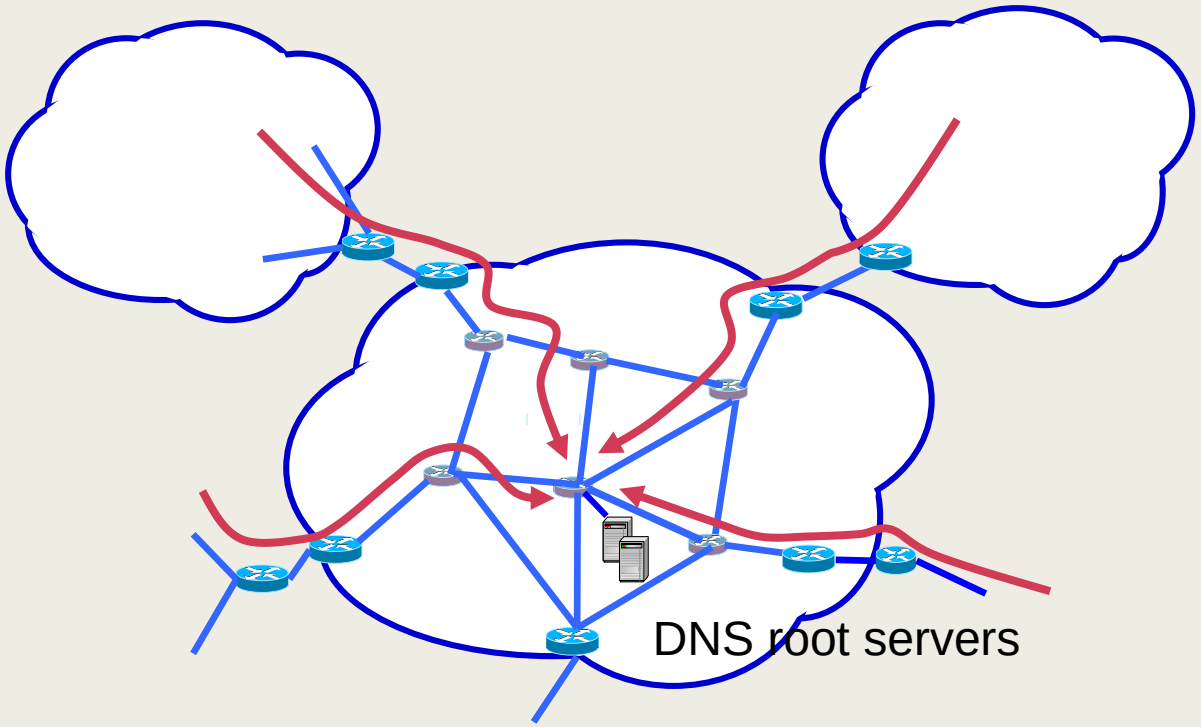
EBay, Amazon, Buy.com hit by attacks

By Martyn Williams
IDG News Service, 02/09/00

A day after the U.S. Web sites of Yahoo were targeted with a denial of service attack, Amazon.com, eBay and Buy.com experienced similar attacks.

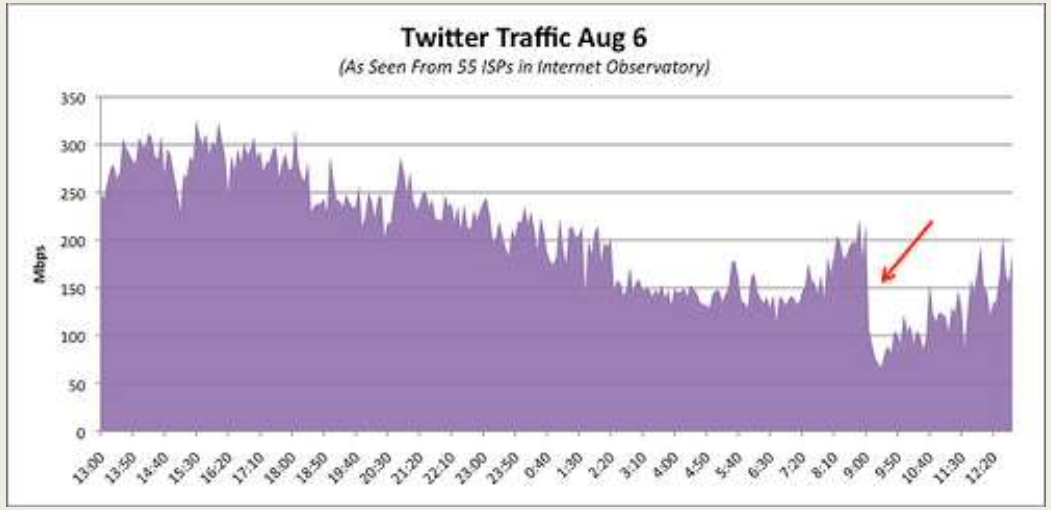
2002 DNS DoS Attacks

- ICMP floods 150 Kpps (primitive attack)
- Took down 7 root servers (two hours)



2009 DDoS on Twitter

- Hours-long service outage
  - *44 million users affected*
- At the same time Facebook, LiveJournal, and YouTube were under attacked
  - *some users experienced an outage*
- Real target: a Georgian blogger



DDoS on Mastercard and Visa

- December 2010
- Targets: MasterCard, Visa, Amazon, Paypal, Swiss Postal Finance, and more

- Attack launched by a group of vigilantes called ***Anonymous*** (~5000 people)
  - DDoS tool is called LOIC or “Low Orbit Ion Cannon”
  - Bots recruited through social engineering
  - Directed to download DDoS software and take instructions from a master
  - Motivation: Payback, due to cut support of WikiLeaks after their founder was arrested on unrelated charges

The new DDoS tool by *Anonymous*

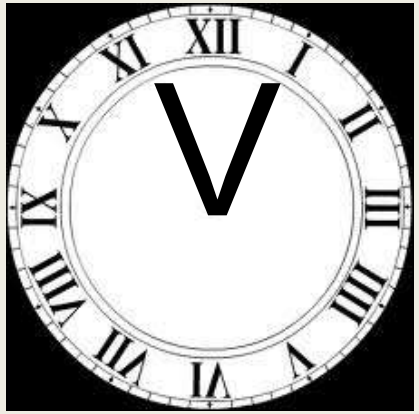
- New operation is beginning
- A successor of LOIC
- Using SQL and .js vulnerability, remotely deface page
- May be available in this September 2011

V for Vendetta

Operation Facebook

- Announcement on YouTube to bomb Facebook on Nov. 5 2011
- Facebook's privacy reveals issues

- **Why Nov. 5?**



Remember Remember poem

Remember remember the fifth of November Gunpowder, treason and plot. I see no reason why gunpowder, treason Should ever be forgot...

DDoS Attack Classification

DOS attack list

- **Flood attack**
  - *TCP SYN flood*
  - *UDP flood*
  - *ICMP (PING) flood*
  - *Amplification (Smurf, Fraggle since 1998)*
- **Vulnerability attack**
  - *Ping of Death (since 1990)*
  - *Tear Drop (since 1997)*
  - *Land (since 1997)*

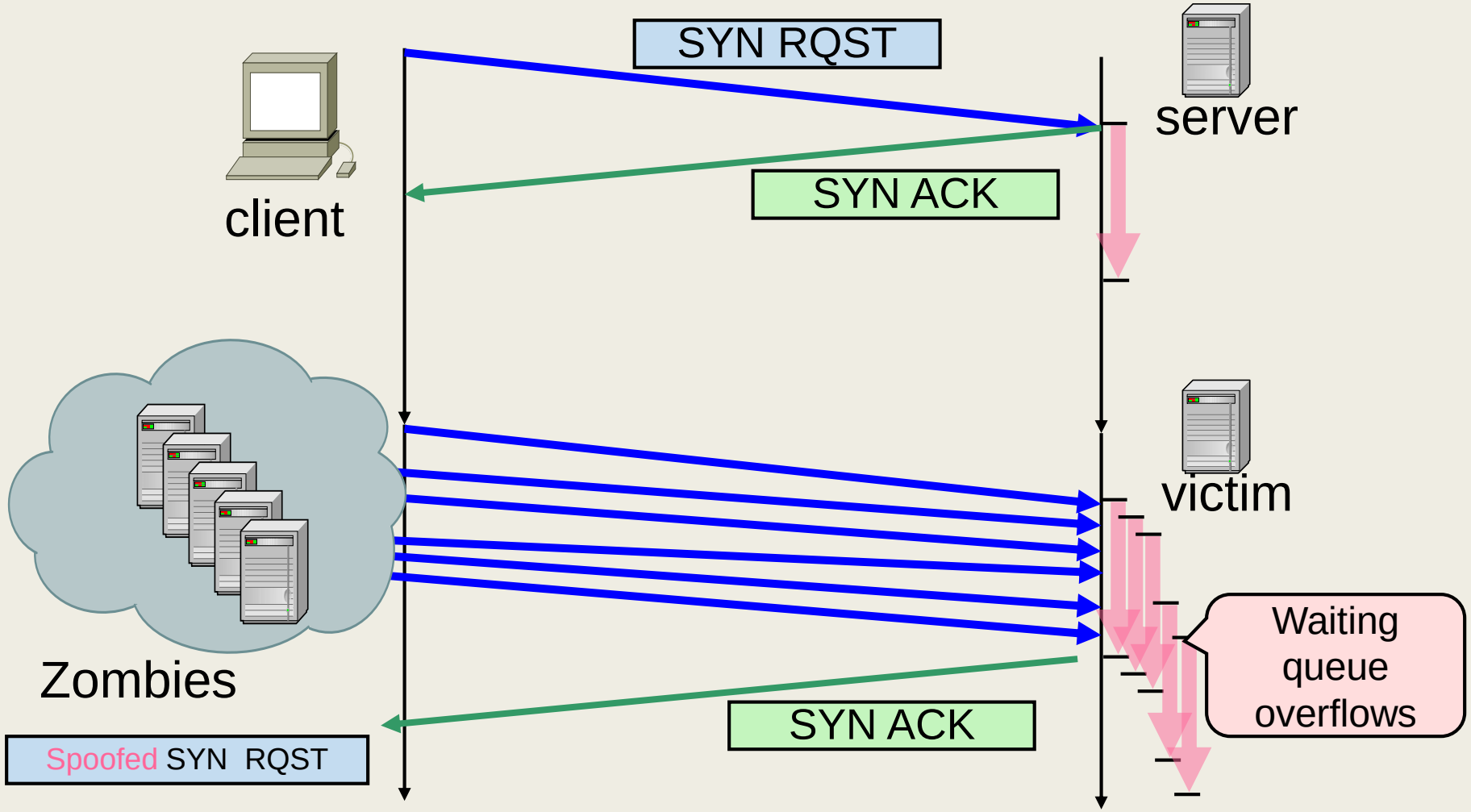
Flooding attack

- Commonly used DDoS attack
- Sending a vast number of messages whose processing consumes some key resource at the target
- The strength lies in the volume, rather than the content
- Implications :
  - The traffic look **legitimate**
  - **Large** traffic flow **large** enough to consume victim's resources
  - **High packet rate** sending

Vulnerability DoS attack

- *Vulnerability* : a bug in implementation or a bug in a default configuration of a service
- *Malicious messages* (exploits) : unexpected input that utilize the vulnerability are sent
- Consequences :
  - The system slows down or crashes or freezes or reboots
  - Target application goes into infinite loop
  - Consumes a vast amount of memory

TCP SYN flood

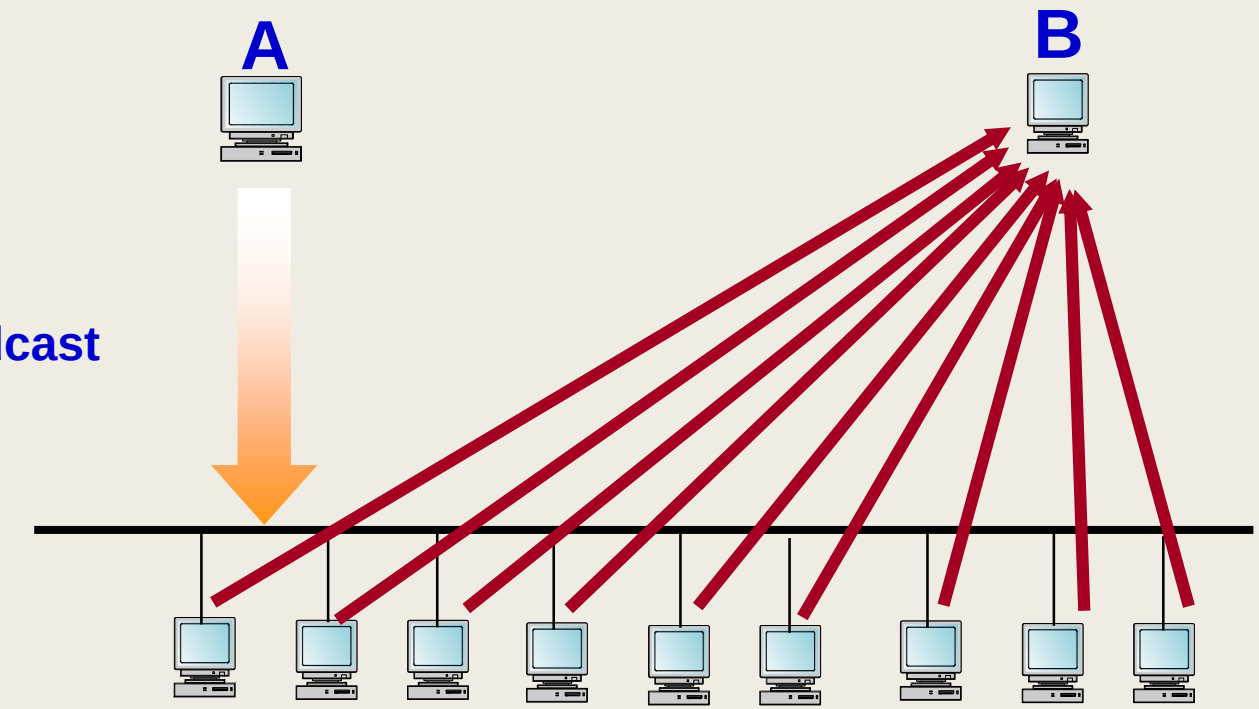


Smurf attack

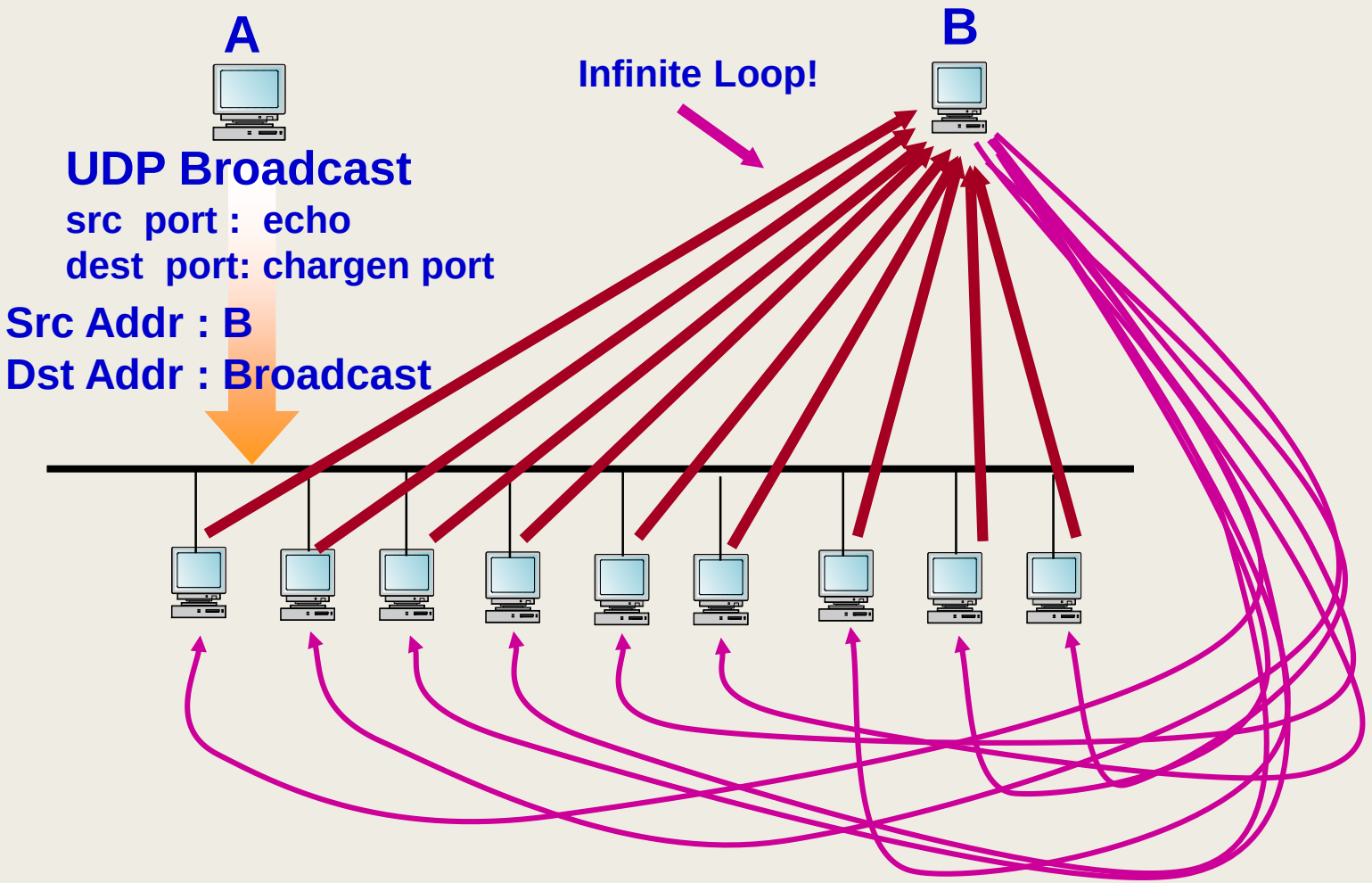
- Amplification attack
  - *Sends ICMP ECHO to network*
  - *Amplified network flood*
  - *widespread pings with faked return address (broadcast address)*
  - *Network sends response to victim system*
  - *The "smurf" attack's cousin is called "fraggle", which uses UDP echo packets in the same fashion*

DoS : Smurf

Ping Broadcast
Src Addr : B
Dst Addr : Broadcast



DoS : Fraggle



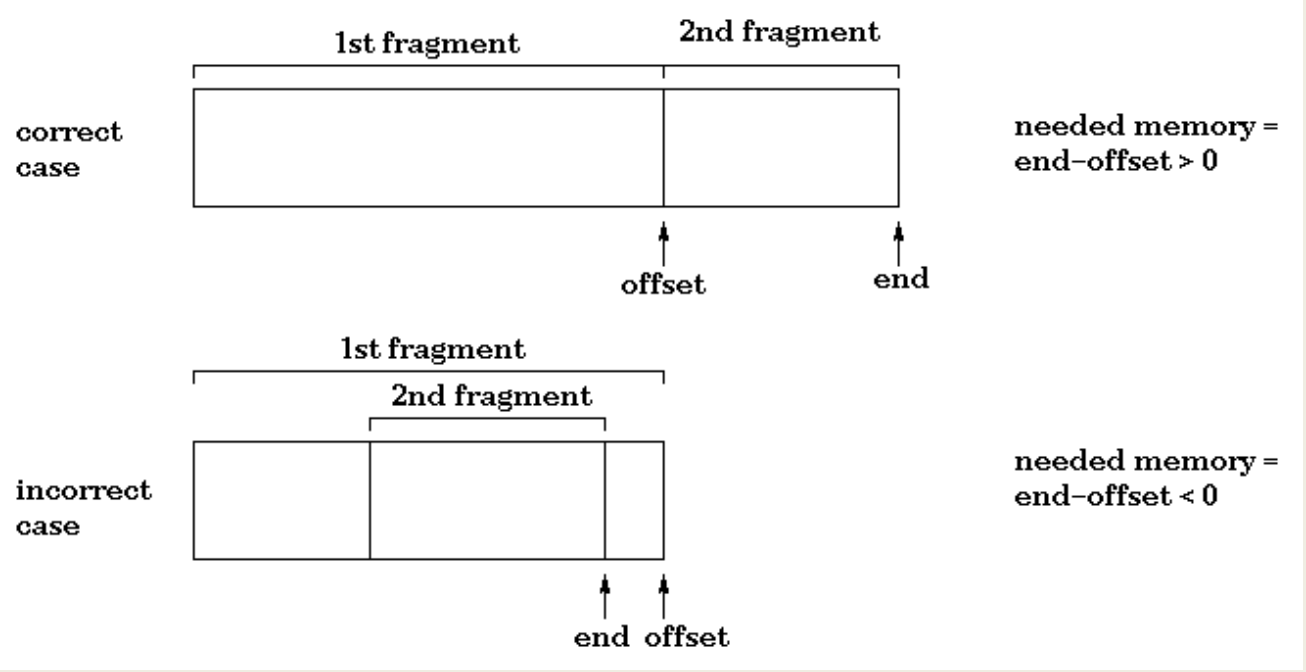
- Well known exploit Echo/Chargen

Ping of Death

- Sending over size ping packet to victim
  - *>65535 bytes ping violates IP packet length*
  - *Causes buffer overflow and system crash*
- Problem in implementation, not protocol
- Has been fixed in modern OSes
  - *Was a problem in late 1990s*

Teardrop

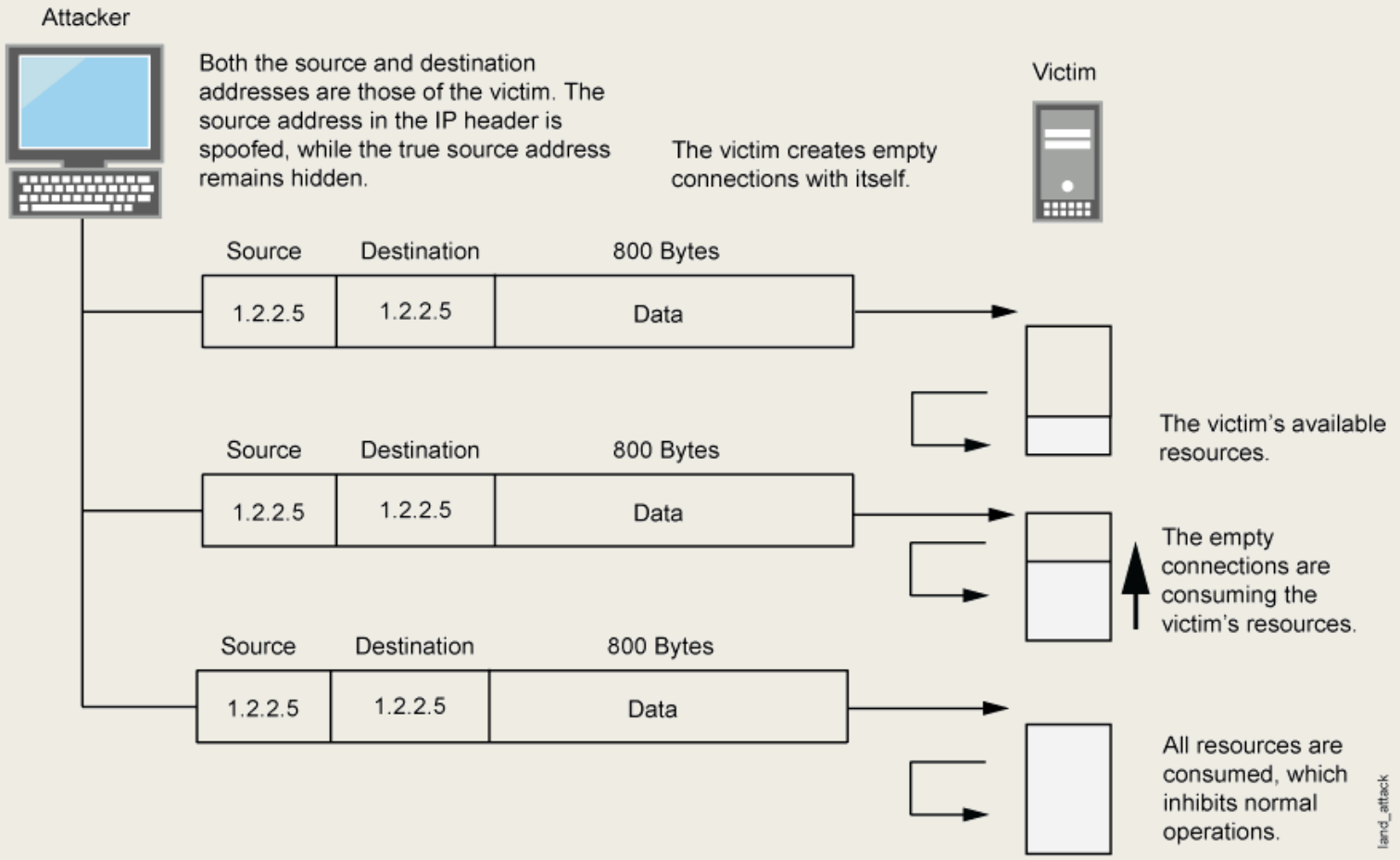
- A bug in their TCP/IP fragment reassembly code
- Mangle IP fragments with overlapping, over-sized payloads to the target machine
- Crash various operating systems



LAND

- A LAND (Local Area Network Denial) attack
- First discovered in 1997 by "m3lt"
  - *Effect several OS :*
    - AIX 3.0
    - FressBSD 2.2.5
    - IBM AS/400 OS7400 3.7
    - Mac OS 7.6.1
    - SUN OS 4.1.3, 4.1.4
    - Windows 95, NT and XP SP2
- IP packets where the source and destination address are set to address the same device
  - *The machine replies to itself continuously*
  - *Published code land.c*

LAND


Attacker
Both the source and destination addresses are those of the victim. The source address in the IP header is spoofed, while the true source address remains hidden.
Victim
The victim creates empty connections with itself.
Source
Destination
800 Bytes
1.2.2.5
1.2.2.5
Data
Source
Destination
800 Bytes
1.2.2.5
1.2.2.5
Data
Source
Destination
800 Bytes
1.2.2.5
1.2.2.5
Data
The victim's available resources.
The empty connections are consuming the victim's resources.
All resources are consumed, which inhibits normal operations.
land_attack

DDoS Defense

Are we safe from DDoS?

- **My machine are well secured**
  - *It does not matter. The problem is not your machine but everyone else*
- **I have a Firewall**
  - *It does not matter. We slip with legitimate traffic or we bomb your firewall*
- **I use VPN**
  - *It does not matter. We can fill your VPN pipe*
- **My system is very high provision**
  - *It does not matter. We can get bigger resource than you have*

Why DoS Defense is difficult

- **Conceptual difficulties**
  - *Mostly random source packet*
  - *Moving filtering upstream requires communication*

- **Practical difficulties**
  - *Routers don't have many spare cycles for analysis/filtering*
  - *Networks must remain stable—bias against infrastructure change*
  - *Attack tracking can cross administrative boundaries*
  - *End-users/victims often see attack differently (more urgently) than network operators*

- **Nonetheless, need to:**
  - *Maximize filtering of bad traffic*
  - *Minimize "collateral damage"*

Defenses against DoS attacks

- DoS attacks cannot be prevented entirely
- Impractical to prevent the **flash crowds** without compromising network performance
- Three lines of defense against (D)DoS attacks
  - *Attack prevention and preemption*
  - *Attack detection and filtering*
  - *Attack source traceback and identification*

Attack prevention

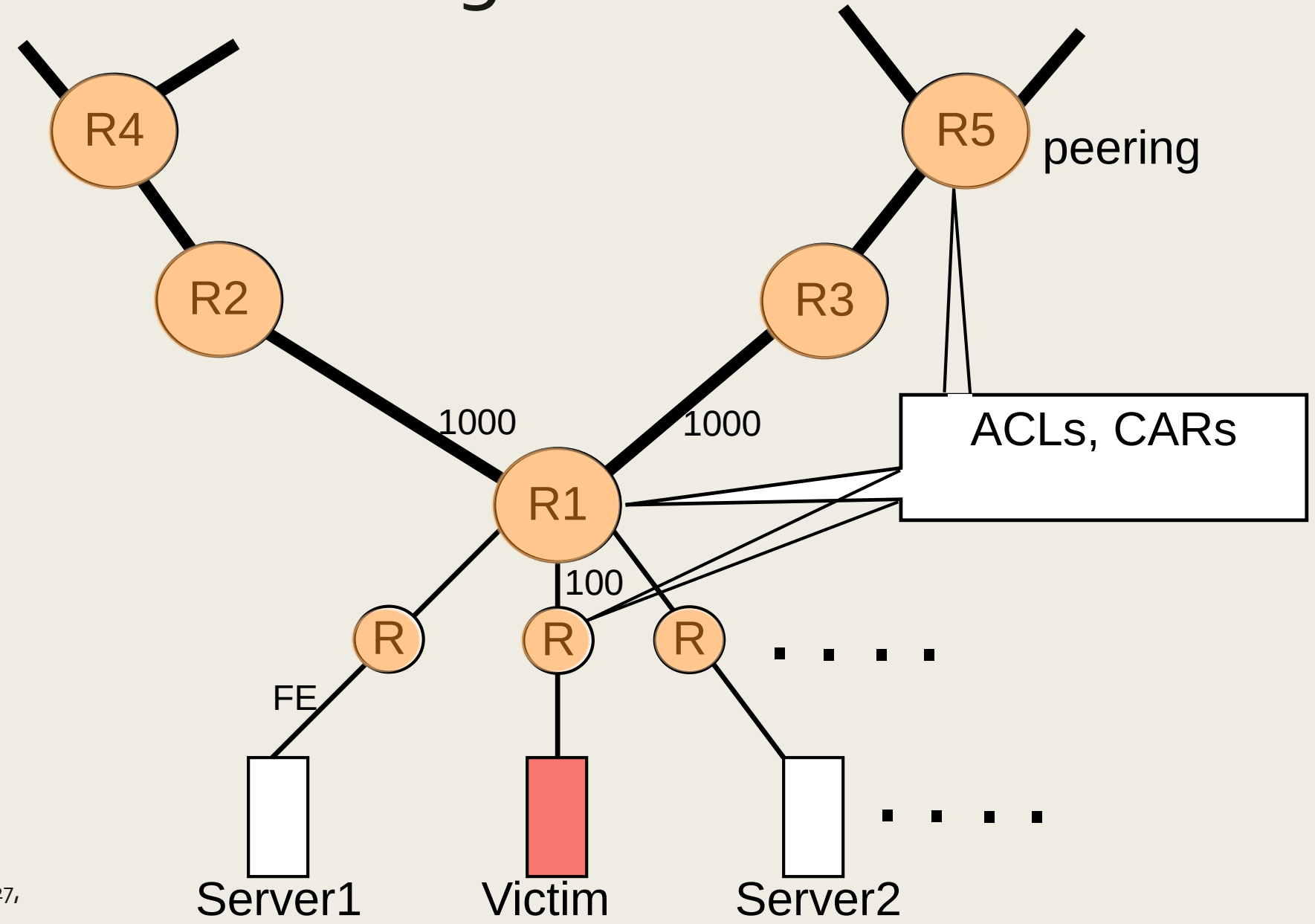
- Limit ability of systems to send spoofed packets
  - *Filtering done as close to source as possible by routers/gateways*
  - *Reverse-path filtering ensure that the path back to claimed source is same as the current packet's path*
    - Ex: On Cisco router "ip verify unicast reverse-path" command
- Rate controls in upstream distribution nets
  - *On specific packet types*
  - *Ex: Some ICMP, some UDP, TCP/SYN*
- Block IP broadcasts

Responding to attacks

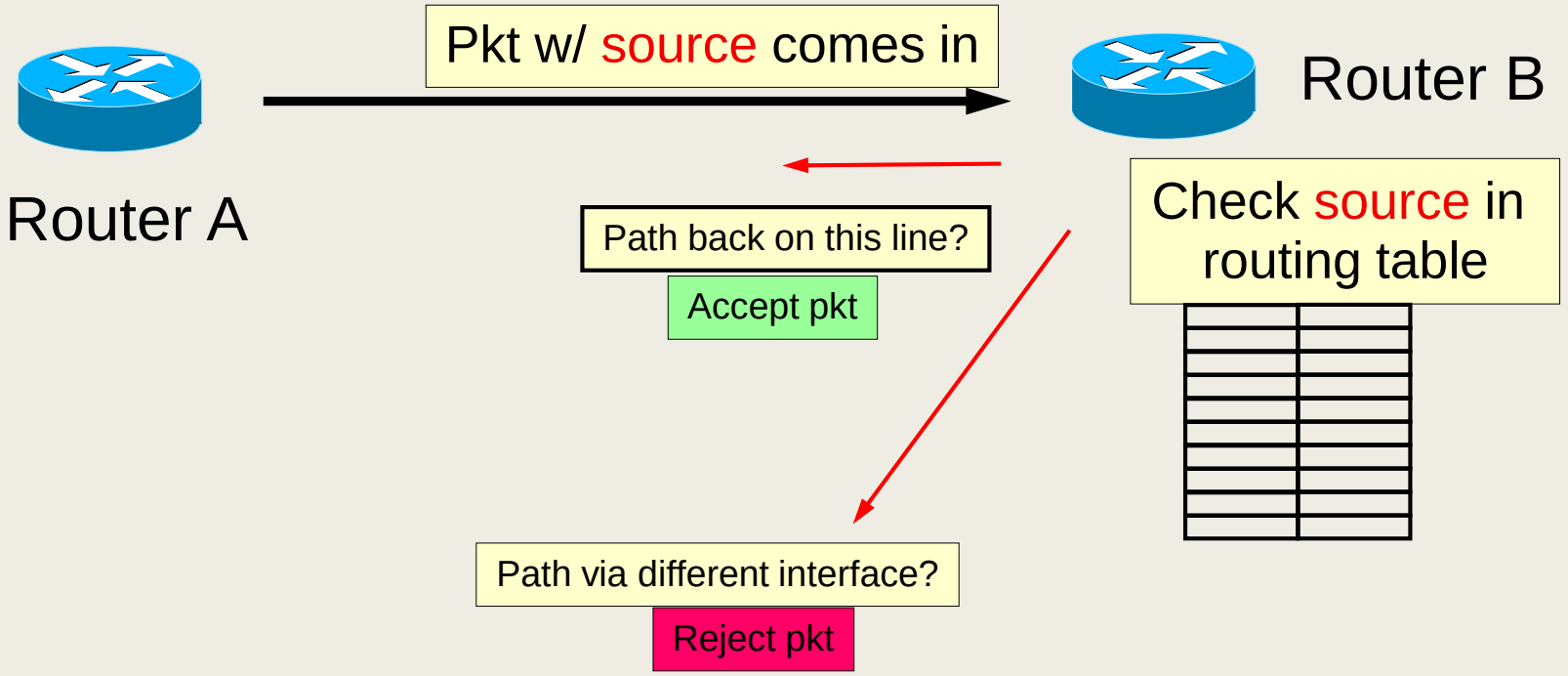
- Need good incident response plan
  - *With contacts for ISP*
  - *Needed to impose traffic filtering upstream*
  - *Details of response process*
- Ideally have network monitors and IDS
  - *To detect and notify abnormal traffic patterns*

How are DDoS practically handled?

Router Filtering

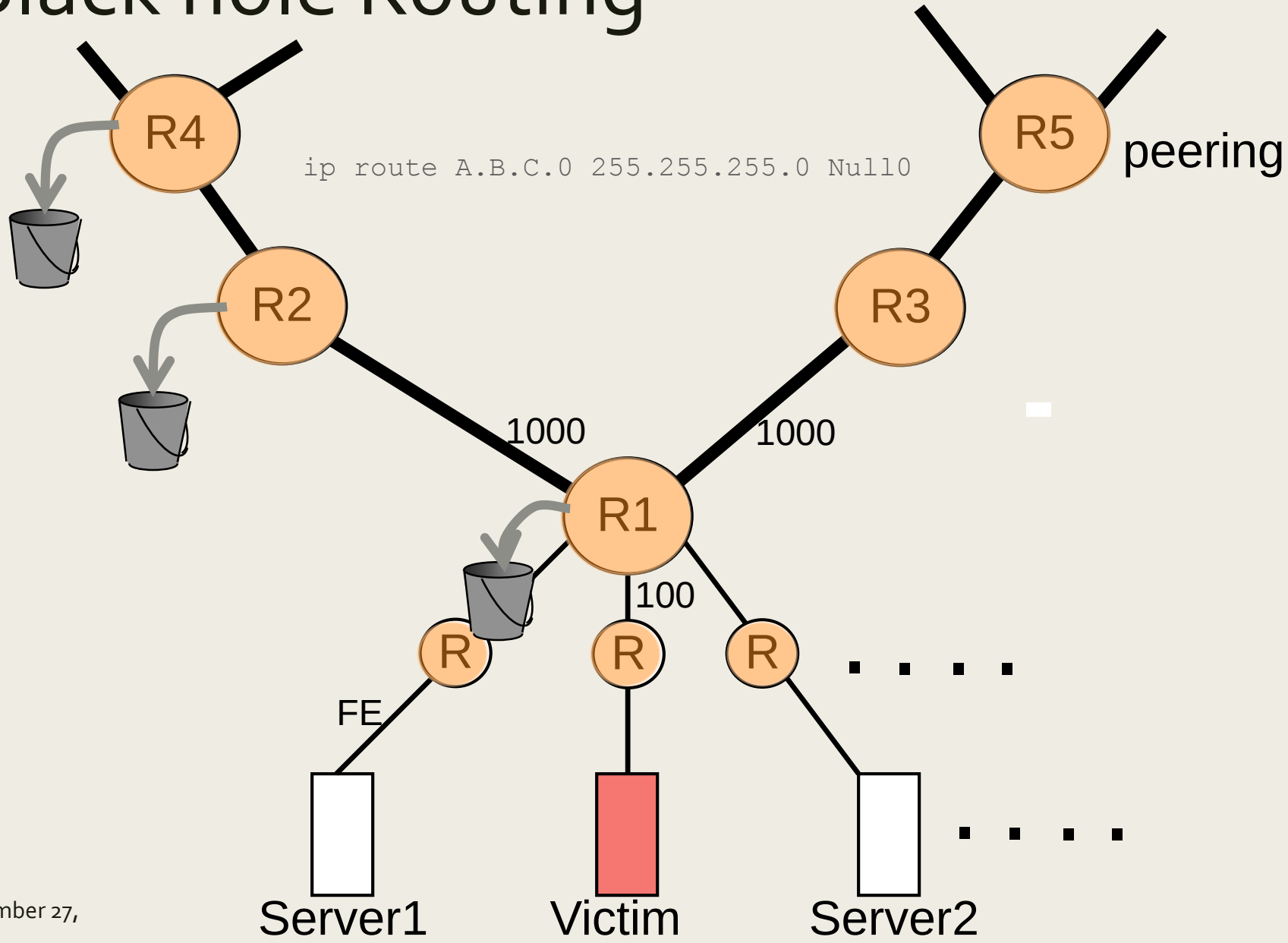


Cisco uRPF

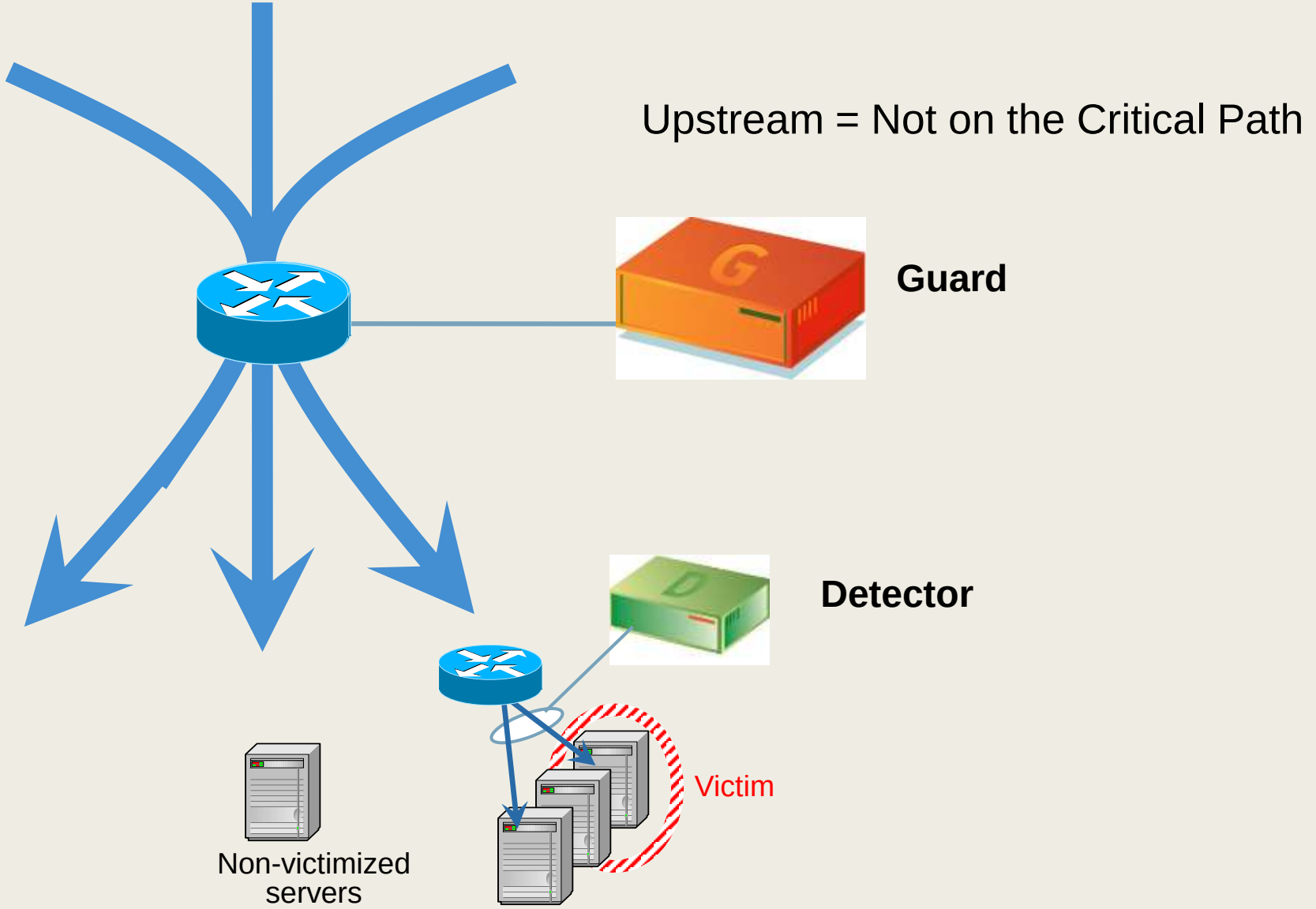


- Unicast Reverse Path Forwarding
- Does routing back to the source go through same interface ?
- Cisco interface command: `ip verify unicast rpf`

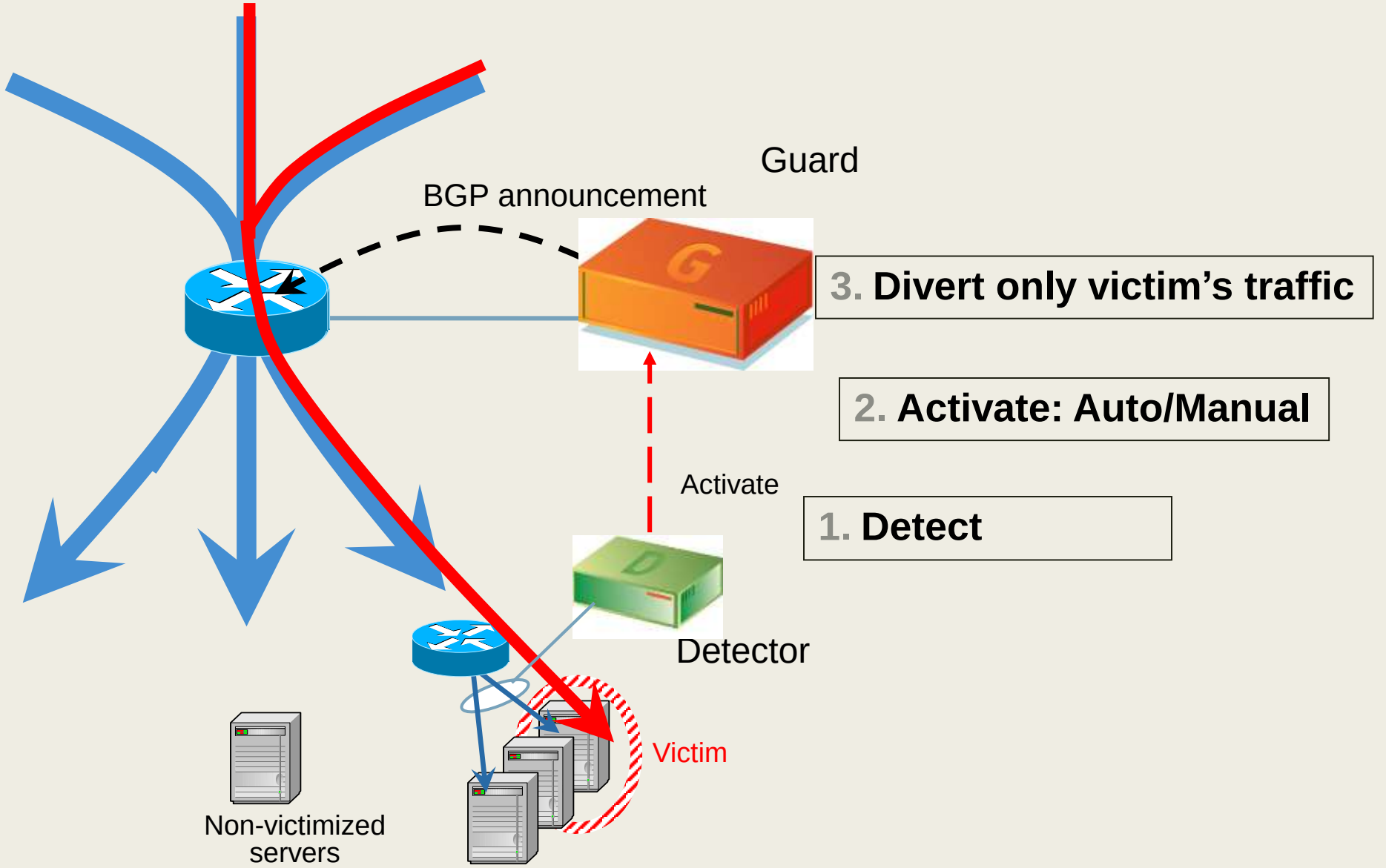
Black hole Routing



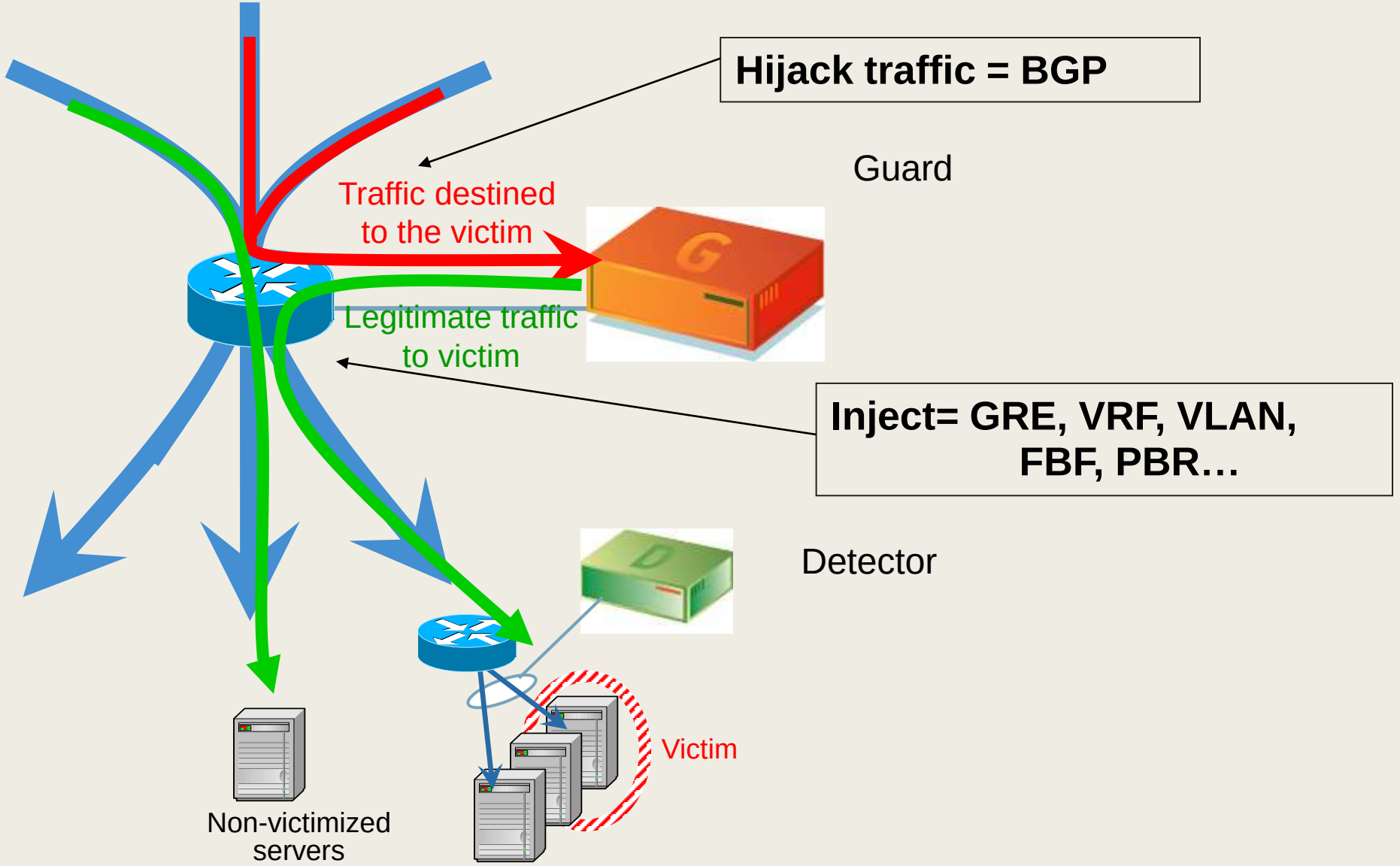
Blackhole in Practice (I)



Blackhole in Practice (II)



Blackhole in Practice (III)



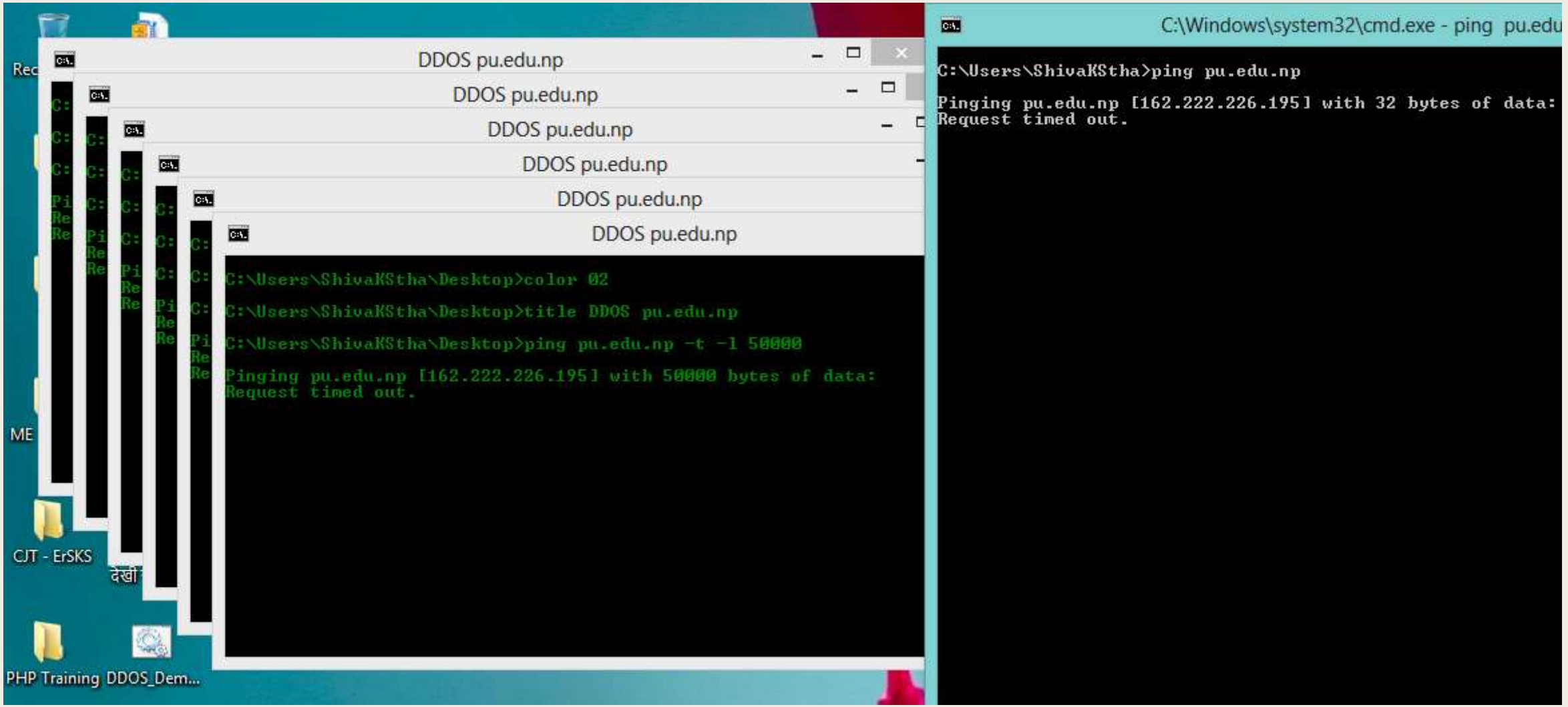
DDoS Attack Trends

- Attackers follow defense approaches, adjust their code to bypass defenses
- Use of subnet spoofing defeats ingress filtering
- Use of encryption and decoy packets, IRC or P2P obscures master-slave communication
- Encryption of attack packets defeats traffic analysis and signature detection
- Pulsing attacks defeat slow defenses and traceback
- Flash-crowd attacks generate application traffic

Conclusion

- No matter how secure a system is or good defense techniques has been used it is not possible to completely prevent DDoS Attack.
- 75 % of Web Application attacks targeted US sites

DoS Attack Demo



- Q/A ?

Thank You !

Recommendations

- http://thehackernews.com/2016/09/ddos-attack-iot.html
- http://www.datacenterdynamics.com/content-tracks/security-risk/ddos-attacks-hit-cloudflare-originate-from-new-botnet/97438.fullarticle
- http://www.theregister.co.uk/2016/12/08/can_isps_step_up_and_solve_the_ddos_problem/
- http://calvinayre.com/2016/12/16/business/bitcoin-exchange-btc-e-falls-victim-ddos-attack/
- http://en.yibada.com/articles/180618/20161222/biggest-hacks-data-breaches-2016-from-yahoo-breach-to-ddos-attacks.htm
- http://news.softpedia.com/news/infographic-ddos-attacks-in-q3-2015-497312.shtml